



COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH
CHIEF INFORMATION OFFICE BUREAU
EFT DATA ACCESS REQUEST FORM

Please Print All Information

Request Type

New ☐

Renewal ☐

Delete ☐

Please note: Your account will expire 1 year from account creation or renewal.

Instructions

Please complete this form in its entirety and return to:

Department of Mental Health
695 S. Vermont Ave., 8th floor
Los Angeles, CA 90005
ATTN: Systems Access Unit

Original Signatures Required. Incomplete forms will NOT be processed.

Applicant Information

Print Applicant Name: _____

Last 4 digits of SSN: _____ Day of Birth: _____ Logon ID: _____

Legal Entity or Provider Number: _____ Legal Entity Provider Name: _____

Telephone Number: _____ E-mail Address: _____

Requestor's Signature: _____ Date: _____

Requesting: Download Access ☐ Upload Access ☐ Confidential Oath & AUP Attached ☐

Authorization

Authorized CEO/Designee Name (Please Print): _____

By signing this form you hereby grant the above employee access to data provided by the Los Angeles County- Department of Mental Health for your organization. This data may include protected Health and/or claiming information, and is subject to protection as required by HIPAA standards and/or guidelines.

CEO/Designee Signature: _____ Date Completed: _____

Contact Person: _____ Phone Number: (____) _____

Contact E-mail: _____

Notice: Upon user termination, it is the Legal Entity's responsibility to notify CIOB via this form. The danger in not terminating the User ID is the user maintains access to your Legal Entity data and the potential to sabotage or misuse client's data exist.

For CIOB Use Only

Approved ☐ Rejected ☐ Remarks: _____ Ticket#: _____

SAU Staff Verified: _____

Date Completed: _____ Date to Network: _____



COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH
CHIEF INFORMATION OFFICE BUREAU
Information Security Division

CONFIDENTIALITY OATH
Non-LAC-DMH Workforce Members

The intent of this Confidentiality Form is to ensure that all County Departments, Contractors, LAC-DMH Non-Governmental Agencies (NGA), Fee-For-Service Hospital (FFS1), Fee-For-Service Outpatient (FFS2) and Pharmacy users are aware of their responsibilities and accountability to protect the confidentiality of clients' sensitive information viewed, maintained and/or accessed by any DMH on-line systems.

Further, the Department's Medi-Cal and MEDS access policy has been established in accordance with Federal and State laws governing confidentiality.

The California Welfare and Institutions (W&I) Code, Section 14100.2, cites the information to be regarded confidential. This information includes applicant/beneficiary names, addresses, services provided, social and economic conditions or circumstances, agency evaluation of personal information, and medical data. (See also 22 California Code of Regulations (C.C.R.), Sections 50111 and 51009)

The Medi-Cal Eligibility Manual, Section 2-H, titled "Confidentiality of Medi-Cal Case Records," referring to Section 14100.2, a, b, f, and h, W&I Code, provides in part that:

- “(a) All types of information, whether written or oral, concerning a person, made or kept by any public office or agency in connection with the administration of any provision of this chapter *... shall be confidential, and shall not be open to examination other than for purposes directly connected with administration of the Medi-Cal program.”
- “(b) Except as provided in this section and to the extent permitted by Federal Law or regulation, all information about applicants and recipients as provided for in subdivision (a) to be safeguarded includes, but is not limited to, names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation or personal information, and medical data, including diagnosis and past history of disease or disability.”
- “(f) The State Department of Health Services may make rules and regulations governing the custody, use and preservation of all records, papers, files, and communications pertaining to the administration of the laws relating to the Medi-Cal program **”
- “(h) Any person who knowingly releases or possesses confidential information concerning persons who have applied for or who have been granted any form of Medi-Cal benefits ***... for which State or Federal funds are made available in violation of this section is guilty of a misdemeanor.”

*, **, *** The State of California's Statute for Medicaid Confidentiality can be found at the following web address: <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/Medicaidstatute.aspx>

The signed copy of this agreement must be maintained by DMH Facilitators

Please read the agreement and take due time to consider it prior to signing.

I understand that County Departments, Contractors, LAC-DMH Non-Governmental Agencies (NGA), Fee-For-Service Hospital (FFS1), Fee-For-Service Outpatient (FFS2) and Pharmacy users are prohibited from sharing their unique Logon I.D. and password with co-worker or other agencies.

Further, I understand that data browsing is strictly prohibited and my access to information is restricted to the minimum necessary required to carry out my job responsibilities.

Further, I understand that County Departments, Contractors, LAC-DMH Non-Governmental Agencies (NGA), Fee-For-Service Hospital (FFS1), Fee-For-Service Outpatient (FFS2) and Pharmacy users are prohibited from obtaining, releasing, or using confidential client information from case records or computer records for purposes not specifically related to the administration of services and authorized by the California Welfare and Institutions Code (Section 14100.2).

Further, I understand the violation of the confidentiality of records or of these policies which are made for protection of the confidentiality of such records, may cause:

1. A civil action under the provision of the Welfare and Institutions Code 5330 Sections:
 - a) Any person may bring an action against an individual who has willfully and knowingly released confidential information or records concerning him or her in violation of this chapter, or of Chapter 1 (commencing with Section 11860) of Part 3 of Division 10.5 of the Health and Safety Code, for the greater of the following amounts:
 1. Ten thousand Dollars (\$10,000)
 2. Three times the amount of actual damages, if any sustained by the plaintiff.
 - b) Any person may bring an action against an individual who has negligently released confidential information or records concerning him or her in violation of this chapter, or of Chapter 1 (commencing with Section 11860) of Part 3 of Division 10.5 of the Health and Safety Code, for both of the following:
 1. One thousand dollars (\$1,000) In order to recover under this paragraph, it shall not be a prerequisite that the plaintiff suffer or be threatened with actual damages.
 2. The amount of actual damages, if any, sustained by the plaintiff
 - c) Any person may, in accordance with Chapter 3(commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin the release of confidential information or records in violation of this chapter, and may in the same action seek damages as provided in this section.
 - d) In addition to the amounts specified in subdivisions (a) and (b), the plaintiff shall recover court costs and reasonable attorney's fees as determined by the court.
2. Disciplinary action including suspension or termination of employment.

Further, I understand that the County will not provide legal protection if violations of these policies or procedures occur.

I hereby certify that I have read this form and I have knowledge of the requirements of State and Federal confidentiality laws and will comply with all applicable provisions of same.

I, the undersigned, hereby agree not to divulge any information or records concerning any client except in accordance with W&I Code, Section 5328 et seq. and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). I acknowledge that the unauthorized release of confidential information as described in this document may result in disciplinary action up to and including termination of any office of employment. I further agree I have read as described in this document that a person may make me subject to a civil action under the provisions of the W&I Code for the unauthorized release of confidential information.

User's Name: _____
Print Signature Date

Phone #: () _____ Ext: _____

Pharmacy, FFS, NGA Legal Entity No. or
Provider #: _____ Provider Name: _____

Address: _____ / _____ / _____
City Zip Code Service Area

**COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE
AND
CONFIDENTIALITY OF
COUNTY INFORMATION TECHNOLOGY RESOURCES
ANNUAL**

As a County of Los Angeles (County) employee, contractor, subcontractor, volunteer, or other authorized user of County information technology (IT) resources, I understand that I occupy a position of trust. Furthermore, I shall use County IT resources in accordance with my Department's policies, standards, and procedures. I understand that County IT resources shall not be used for:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;

I shall maintain the confidentiality of County IT resources (e.g., business information, personal information, and confidential information).

This Agreement is required by Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, which may be consulted directly at website <http://countypolicy.co.la.ca.us/6.101.htm>.

As used in this Agreement, the term "County IT resources" includes, without limitation, computers, systems, networks, software, and data, documentation and other information, owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities for County purposes. The definitions of the terms "County IT resources", "County IT user", "County IT security incident", "County Department", and "computing devices" are fully set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, which may be consulted directly at website <http://countypolicy.co.la.ca.us/6.100.htm>. The terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information, which may be consulted directly at website <http://countypolicy.co.la.ca.us/3.040.htm>.

As a County IT user, I agree to the following:

1. Computer crimes: I am aware of California Penal Code Section 502(c) – Comprehensive Computer Data Access and Fraud Act (set forth, in part, below). I shall immediately report to my management any suspected misuse or crimes relating to County IT resources or otherwise.
2. No Expectation of Privacy: I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I understand that having no expectation to

any right to privacy includes, for example, that my access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.

3. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall not either intentionally, or through negligence, damage, interfere with the operation of County IT resources. I shall neither, prevent authorized access, nor enable unauthorized access to County IT resources responsibly, professionally, ethically, and lawfully.
4. County IT security incident reporting: I shall notify the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as a County IT security incident is suspected.
5. Security access controls: I shall not subvert or bypass any security measure or system which has been implemented to control or restrict access to County IT resources and any related restricted work areas and facilities. I shall not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards).
6. Passwords: I shall not keep or maintain any unsecured record of my password(s) to access County IT resources, whether on paper, in an electronic file, or otherwise. I shall comply with all County and County Department policies relating to passwords. I shall immediately report to my management any compromise or suspected compromise of my password(s) and have the password(s) changed immediately.
7. Business purposes: I shall use County IT resources in accordance with my Department's policies, standards, and procedures.
8. Confidentiality: I shall not send, disseminate, or otherwise expose or disclose to any person or organization, any personal and/or confidential information, unless specifically authorized to do so by County management. This includes, without limitation information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.
9. Computer virus and other malicious devices: I shall not intentionally introduce any malicious device (e.g., computer virus, spyware, worm, key logger, or malicious code), into any County IT resources. I shall not use County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks. I shall not disable, modify, or delete computer security software (e.g., antivirus software, antispymware software, firewall software, and host intrusion prevention software) on County IT resources. I shall notify the County Department's Help Desk and/or DISO as soon as any item of County IT resources is suspected of being compromised by a malicious device.

10. Offensive materials: I shall not access, create, or distribute (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on County IT resources.
11. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services in accordance with my Department's policies and procedures. I understand that my use of the County Internet services may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall comply with all County Internet use policies, standards, and procedures. I understand that County Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.
12. Electronic Communications: I understand that County electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such electronic communications may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time, without notice or consent. I shall comply with all County electronic communications use policies and use proper business etiquette when communicating over County electronic communications systems/applications/services.
13. Public forums: I shall only use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with Department's policies, standards, and procedures.
14. Internet storage sites: I shall not store County information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data)) on any Internet storage site in accordance with Department's policies, standards, and procedures.
15. Copyrighted and other proprietary materials: I shall not copy or otherwise use any copyrighted or other proprietary County IT resources (e.g., licensed software and documentation, and data), except as permitted by the applicable license agreement and approved by designated County Department management. I shall not use County IT resources to infringe on copyrighted material.
16. Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No.

6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

17. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision of this Agreement may result in disciplinary action and other actions (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

**CALIFORNIA PENAL CODE SECTION 502(c)
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"**

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code Section 502(c) is incorporated in its entirety into this Agreement by reference, and all provisions of Penal Code Section 502(c) shall apply. For a complete copy, consult the Penal Code directly at website www.leginfo.ca.gov/.

502(c) Any person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

County IT User's Name

County IT User's Signature

County IT User's Employee/ID Number

Date

Manager's Name

Manager's Signature

Manager's Title

Date